Terbit online pada laman web jurnal : https://pkm.unrida.ac.id/index.php/GLOBALENT

GLOBALENT: Journal of Global Entrepreneurial Community Service

Artikel Pengabdian Kepada Masyarakat

Legalitas dan Perlindungan Hukum Data Biometrik Pengguna Aplikasi Paylater di Indonesia dalam Perspektif UU PDP

Imeldalius*[1], Yuda Dibrata[2], Henry Halim[3], Novrida Fauziyah Nasution[4]

1 Program Studi Ilmu Hukum, Fakultas Hukum, Sekolah Tinggi Ilmu Hukum, Indonesia
2 Program Studi Ilmu Hukum, Fakultas Hukum, Sekolah Tinggi Ilmu Hukum, Indonesia
3 Program Studi Ilmu Hukum, Fakultas Hukum, Sekolah Tinggi Ilmu Hukum, Indonesia
4 Program Studi Ilmu Hukum, Fakultas Hukum, Sekolah Tinggi Ilmu Hukum, Indonesia

E-mail: imeldalius@stih.ac.id, yudadibrata@stih.ac.id, henryhalim@stih.ac.id, novridafauziyah@stih.ac.id

INFORMASI ARTIKEL

Volume 1 Issue 1
Received: 29 Agustus 2022
Accepted: 10 Oktober 2022
Publish 31 Desember 2022

Online:
https://pkm.unrida.ac.id/index.php/GLOBALENT

Kata Kunci
Data biometrik
Paylater
UU PDP
Perlindungan hukum
Literasi hukum digital

A B S T R A K

Penggunaan aplikasi paylater mendorong verifikasi identitas digital yang semakin intensif, termasuk pengambilan foto wajah, swafoto, dan unsur biometrik lain untuk proses e-KYC dan pengendalian risiko kredit. Kondisi tersebut menimbulkan kebutuhan literasi hukum karena data biometrik merupakan data pribadi bersifat spesifik yang memerlukan perlindungan lebih kuat berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Artikel pengabdian ini menyajikan rancangan program edukasi dan pendampingan hukum bagi pengguna atau calon pengguna paylater agar mampu memahami legalitas pemrosesan data biometrik, hak sebagai subjek data pribadi, kewajiban pengendali data, serta mekanisme pencegahan dan penanganan penyalahgunaan data. Metode kegiatan menggunakan pendekatan penyuluhan partisipatif, studi kasus, simulasi pemeriksaan izin akses aplikasi, klinik konsultasi, serta evaluasi pre-test dan post-test. Luaran kegiatan berupa modul ringkas, checklist kepatuhan pengguna, model alur pengaduan, dan rekomendasi tata kelola data berbasis privacy by design. Program ini diharapkan memperkuat kesadaran hukum digital masyarakat dan mendorong ekosistem paylater yang transparan, proporsional, aman, dan akuntabel.

Catatan penyesuaian naskah: identitas penulis, nama mitra, lokasi, tanggal, jumlah peserta, dan angka hasil evaluasi dalam draf ini perlu diisi atau disesuaikan dengan data kegiatan PKM yang benar-benar dilaksanakan sebelum naskah disubmit ke jurnal.

1. Pendahuluan

Transformasi layanan keuangan digital telah mengubah cara masyarakat memperoleh fasilitas pembiayaan konsumtif. Paylater atau buy now, pay later (BNPL) menyediakan mekanisme pembelian barang atau jasa dengan pembayaran tertunda atau cicilan, sehingga layanan ini dekat dengan aktivitas e-commerce, dompet digital, dan platform keuangan berbasis aplikasi. Secara konseptual, paylater memiliki karakteristik yang berbeda dari kredit perbankan konvensional karena proses registrasi, penilaian kelayakan, pemberian limit, dan pemantauan risiko dilakukan secara elektronik dengan dukungan data digital pengguna (Novendra & Aulianisa, 2020). Perkembangan BNPL juga dipengaruhi oleh meningkatnya transaksi e-commerce dan preferensi konsumen terhadap pembayaran yang cepat, fleksibel, dan mudah diakses (Cornelli et al., 2023; Kumar et al., 2024).

Kemudahan tersebut tidak terlepas dari kebutuhan verifikasi identitas. Dalam praktik aplikasi paylater, pengguna sering diminta mengunggah kartu identitas, foto wajah, swafoto memegang identitas, rekaman liveness detection, nomor ponsel, kontak darurat, informasi pekerjaan, dan data keuangan pribadi. Sebagian

proses verifikasi memanfaatkan unsur biometrik karena ciri fisik seperti wajah, sidik jari, atau pola suara dapat digunakan untuk mengenali atau memverifi`kasi identitas seseorang. Data biometrik memiliki nilai perlindungan yang lebih tinggi dibandingkan kata sandi karena bersifat unik, melekat pada individu, dan sulit atau bahkan tidak mungkin diganti apabila bocor (Sembiring et al., 2024; Melzi et al., 2024).

Dalam perspektif hukum Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menempatkan data biometrik sebagai data pribadi yang bersifat spesifik. Artinya, pemrosesan data biometrik tidak cukup hanya dinilai dari adanya fitur aplikasi, tetapi harus diuji berdasarkan asas, dasar pemrosesan, tujuan yang spesifik, transparansi, keamanan, akuntabilitas, serta penghormatan terhadap hak subjek data pribadi (Republik Indonesia, 2022; Syailendra et al., 2024). Dengan demikian, legalitas penggunaan data biometrik pada aplikasi paylater bertumpu pada kejelasan dasar pemrosesan, kesesuaian tujuan, kewajaran jumlah data yang dikumpulkan, serta adanya langkah pengamanan yang sepadan dengan risiko.

Permasalahan yang dihadapi masyarakat sebagai pengguna paylater bukan hanya risiko gagal bayar, tetapi juga risiko penyalahgunaan identitas digital. Beberapa kajian menemukan bahwa transaksi paylater dan pinjaman online masih memunculkan persoalan perlindungan data pribadi, termasuk kurangnya pemahaman konsumen terhadap pemberian persetujuan, akses aplikasi terhadap data, serta mekanisme pengaduan ketika data disalahgunakan (Fadhli et al., 2022; Gunawan, 2024; Kim et al., 2025). Pada saat yang sama, Otoritas Jasa Keuangan mulai memperkuat kerangka pengaturan BNPL untuk meningkatkan kepastian hukum, tata kelola, manajemen risiko, perlindungan konsumen, dan perkembangan industri yang sehat (Otoritas Jasa Keuangan, 2025).

Urgensi kegiatan pengabdian kepada masyarakat muncul karena literasi hukum digital belum selalu sejalan dengan kecepatan adopsi teknologi finansial. Pengguna muda, mahasiswa, pekerja awal karier, pelaku UMKM, dan masyarakat umum sering menggunakan paylater karena kemudahan proses, promosi, dan fleksibilitas pembayaran. Namun, pemahaman terhadap konsekuensi hukum pemberian data biometrik, hak untuk menarik persetujuan, hak akses, hak perbaikan, hak penghapusan, serta hak menggugat ganti rugi masih perlu diperkuat. Kajian terhadap generasi Z menunjukkan bahwa paylater dipersepsikan bermanfaat dalam transaksi digital, tetapi tetap membutuhkan edukasi pengelolaan risiko agar tidak menimbulkan beban finansial dan risiko data pribadi (Sitepu & Fadila, 2024).

Berdasarkan analisis situasi tersebut, artikel ini merumuskan program PKM berupa edukasi dan pendampingan hukum tentang legalitas serta perlindungan data biometrik pengguna aplikasi paylater dalam perspektif UU PDP. Tujuan kegiatan adalah: (1) meningkatkan pengetahuan peserta mengenai status hukum data biometrik; (2) melatih peserta mengevaluasi legalitas pemrosesan data biometrik pada aplikasi paylater; (3) memberikan keterampilan praktis untuk membaca kebijakan privasi, mengatur izin akses perangkat, dan menyimpan bukti transaksi; serta (4) memperkenalkan langkah preventif dan represif ketika terjadi penyalahgunaan data pribadi. Manfaat kegiatan diharapkan tidak hanya dirasakan oleh peserta, tetapi juga oleh komunitas mitra melalui terbentuknya budaya sadar data, kehati-hatian digital, dan kemampuan menggunakan kanal pengaduan secara tepat.

2. Kajian Terdahulu

Kajian tentang data biometrik menunjukkan bahwa perlindungan tidak dapat hanya mengandalkan persetujuan formal. Sembiring et al. (2024) menekankan bahwa data biometrik memerlukan pelindungan yang lebih ketat karena karakteristiknya yang unik dan tidak mudah dipertukarkan. Pendekatan privacy by design menjadi penting agar perlindungan privasi dipikirkan sejak tahap perancangan sistem, bukan baru diterapkan setelah terjadi pelanggaran. Dalam konteks teknis, Melzi et al. (2024) mengulas berbagai privacy-enhancing technologies untuk sistem biometrik, seperti template protection, enkripsi, pseudonimisasi, dan mekanisme pembatasan pemrosesan yang bertujuan mengurangi risiko identifikasi berlebihan.

Kajian mengenai UU PDP memperlihatkan bahwa Indonesia telah memasuki babak baru perlindungan data pribadi, tetapi implementasinya masih menuntut kesiapan kelembagaan, kepatuhan pelaku usaha, dan literasi masyarakat. Syailendra et al. (2024) menilai bahwa UU PDP merupakan langkah penting dalam memperkuat perlindungan warga negara, namun masih terdapat tantangan dalam penerapan prinsip, pengawasan, dan penegakan hukum. Tantangan tersebut relevan dengan sektor paylater karena layanan ini memproses data yang beragam, berskala besar, dan terkait langsung dengan profil risiko keuangan pengguna.

Penelitian pada sektor pinjaman online dan paylater memperkuat relevansi program pengabdian ini. Fadhli et al. (2022) membahas perlindungan data pribadi konsumen dalam transaksi paylater dan

menempatkan persetujuan pengguna sebagai unsur penting dalam penggunaan data pribadi. Gunawan (2024) menganalisis upaya preventif dan represif terhadap kebocoran data dalam penyelenggaraan pinjaman online, termasuk gagasan pemanfaatan teknologi biometrik sebagai verifikasi yang lebih aman. Kim et al. (2025) menunjukkan bahwa perlindungan data pada platform pinjaman online harus dikaitkan dengan tanggung jawab pengendali data dan hak konsumen menurut UU PDP. Safriadi (2025) juga menegaskan bahwa kebocoran data pribadi dalam ekosistem e-commerce dan paylater berhubungan dengan aspek hak asasi manusia dan tanggung jawab ganti rugi.

Pada sisi teknologi aplikasi, Ramadhani et al. (2023) mengkaji pemanfaatan kecerdasan buatan pada fitur paylater dan kaitannya dengan data pribadi konsumen. Penggunaan AI untuk verifikasi, scoring, dan personalisasi layanan meningkatkan efisiensi, tetapi sekaligus menuntut transparansi dan pembatasan tujuan agar pemrosesan data tidak melampaui kebutuhan. Kajian BNPL secara global juga menunjukkan perlunya kerangka regulasi yang adaptif karena BNPL tumbuh cepat di negara dengan e-commerce kuat, namun dapat menimbulkan risiko keterlambatan pembayaran, over-indebtedness, dan ketidakjelasan pelaporan kredit (Cornelli et al., 2023; Irawati et al., 2024).

Kegiatan PKM terkait perlindungan data pribadi sudah dilakukan dalam beberapa konteks. Bangun et al. (2023) menunjukkan bahwa sosialisasi perlindungan data pribadi sebagai bagian dari hak asasi manusia dapat meningkatkan pemahaman masyarakat. Candiwan et al. (2025) menggunakan model pre-test, sosialisasi, diskusi, dan post-test dalam pelatihan UU PDP untuk guru dan melaporkan peningkatan pemahaman peserta. Berdasarkan kajian tersebut, kebaruan program ini terletak pada fokus yang lebih spesifik, yaitu literasi hukum data biometrik pada aplikasi paylater. Fokus ini menggabungkan isu perlindungan data spesifik, transaksi pembiayaan digital, AI/e-KYC, dan keterampilan praktis pengguna dalam mengelola risiko hukum.

3. Metodologi Penelitian

Metode yang digunakan dalam artikel pengabdian ini adalah edukasi hukum partisipatif dengan pendekatan problem based learning. Kegiatan dirancang untuk dilaksanakan pada komunitas pengguna atau calon pengguna paylater di lingkungan [nama mitra], misalnya mahasiswa, komunitas pemuda, pelaku UMKM, atau masyarakat urban yang aktif menggunakan aplikasi e-commerce. Lokasi kegiatan, tanggal pelaksanaan, jumlah peserta, dan profil mitra perlu diisi sesuai pelaksanaan nyata. Secara substansial, program menyasar peserta yang memiliki pengalaman menggunakan paylater atau setidaknya pernah melalui proses registrasi aplikasi keuangan digital yang meminta verifikasi identitas.

Mitra kegiatan berperan sebagai penyedia peserta, tempat atau ruang pertemuan, serta fasilitator tindak lanjut. Tim pelaksana berperan menyiapkan modul hukum, instrumen evaluasi, studi kasus, lembar checklist, dan materi visual. Kegiatan dilaksanakan melalui empat tahap, yaitu persiapan, pelaksanaan, evaluasi, dan tindak lanjut. Tahap persiapan meliputi identifikasi kebutuhan mitra, pemetaan masalah hukum yang sering muncul, penyusunan modul, serta penyiapan pre-test dan post-test. Tahap pelaksanaan meliputi pemaparan materi, diskusi kasus, simulasi cek legalitas aplikasi, dan klinik konsultasi. Tahap evaluasi dilakukan melalui pembandingan hasil pre-test dan post-test, observasi partisipasi, serta umpan balik peserta. Tahap tindak lanjut menghasilkan checklist penggunaan paylater aman dan rekomendasi kanal pengaduan.

Materi kegiatan dibagi menjadi lima pokok bahasan. Pertama, pengenalan data pribadi dan data biometrik menurut UU PDP. Kedua, legalitas pemrosesan data biometrik pada aplikasi paylater, meliputi persetujuan, tujuan spesifik, transparansi, pembatasan pemrosesan, dan keamanan. Ketiga, hak subjek data pribadi, termasuk hak memperoleh informasi, hak akses, hak koreksi, hak penghapusan, hak menarik persetujuan, dan hak menuntut ganti rugi. Keempat, kewajiban pengendali dan prosesor data pribadi, khususnya kewajiban menjaga keamanan, melakukan penilaian risiko, membatasi retensi, serta memberi pemberitahuan jika terjadi kegagalan perlindungan data. Kelima, simulasi perlindungan mandiri, seperti membaca privacy notice, memeriksa izin kamera dan kontak, menyimpan bukti persetujuan, dan menghindari unggahan data biometrik ke pihak yang tidak terverifikasi.

Teknik pengumpulan data evaluasi menggunakan kuesioner pre-test dan post-test, observasi, dokumentasi kegiatan, dan lembar umpan balik peserta. Instrumen pre-test dan post-test disusun dalam bentuk pilihan ganda dan studi kasus singkat yang menilai tiga aspek: pengetahuan hukum, keterampilan identifikasi risiko, dan sikap kehati-hatian. Indikator keberhasilan program adalah peningkatan skor pemahaman, kemampuan peserta menjelaskan minimal tiga hak subjek data pribadi, kemampuan peserta

mengidentifikasi legalitas pemrosesan data biometrik, dan kemampuan peserta menyusun langkah pengaduan awal apabila terjadi penyalahgunaan data.

Tabel 1. Rancangan Tahapan Program PKM

Tahap	Kegiatan Utama	Luaran	Indikator Keberhasilan
Persiapan	Identifikasi kebutuhan mitra, telaah regulasi, penyusunan modul, penyusunan instrumen pre-test dan post-test.	Modul ringkas, kuesioner, studi kasus, dan checklist awal.	Materi tervalidasi oleh tim dan mitra; instrumen siap digunakan.
Pelaksanaan	Penyuluhan UU PDP, diskusi kasus paylater, simulasi cek izin akses aplikasi, dan klinik konsultasi.	Dokumentasi kegiatan, daftar hadir, dan catatan pertanyaan peserta.	Peserta aktif bertanya dan mampu mengaitkan kasus dengan hak serta kewajiban hukum.
Evaluasi	Pengisian post-test, refleksi, dan pengumpulan umpan balik.	Rekap skor, testimoni peserta, dan peta kebutuhan lanjutan.	Terjadi peningkatan skor pemahaman dan muncul rekomendasi tindak lanjut.
Tindak lanjut	Penyusunan panduan ringkas dan pendampingan komunikasi pengaduan awal jika diperlukan.	Checklist aman menggunakan paylater dan template kronologi aduan.	Mitra memiliki bahan edukasi yang dapat digunakan ulang.

3.1 Rumus Metode Penelitian

Efektivitas kegiatan dapat dihitung dengan membandingkan skor pre-test dan post-test. Rumus yang digunakan adalah sebagai berikut:

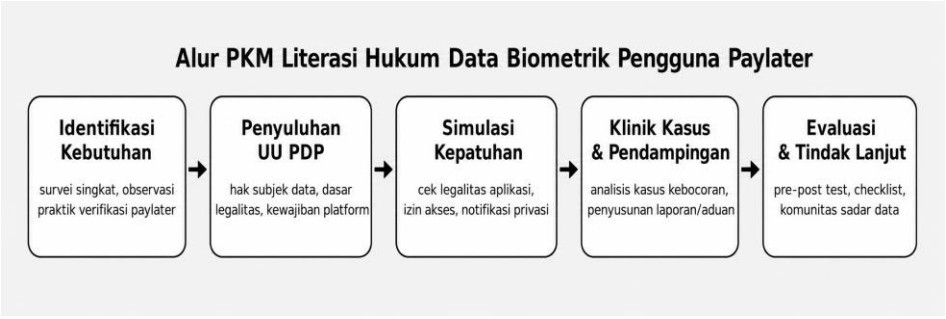
Skor Pemahaman (%) = (Jumlah jawaban benar / Jumlah soal) x 100
N-Gain = (Skor post-test - Skor pre-test) / (100 - Skor pre-test)

Rumus tersebut membantu tim menilai perubahan pemahaman peserta secara lebih objektif. Interpretasi hasil dapat dibuat dalam kategori rendah, sedang, dan tinggi sesuai kebutuhan penulis. Apabila jurnal meminta data kuantitatif, bagian ini dapat dilengkapi dengan jumlah peserta, rata-rata skor, deviasi standar, dan persentase peningkatan.

3.2 Visual Table & Gambar

Tabel 2. Contoh Instrumen Evaluasi Pemahaman Peserta

Aspek Evaluasi	Contoh Pertanyaan/Indikator	Skor Pre-test	Skor Post-test	Keterangan
Pengetahuan hukum	Peserta mengetahui bahwa data biometrik termasuk data pribadi spesifik dalam UU PDP.	50	90	Diukur dengan pilihan ganda.
Keterampilan identifikasi risiko	Peserta dapat menilai apakah permintaan akses kamera, kontak, dan foto wajah relevan dengan tujuan layanan.	50	90	Diukur dengan studi kasus.
Sikap kehati-hatian	Peserta bersedia membaca kebijakan privasi, menyimpan bukti persetujuan, dan tidak membagikan OTP atau swafoto ke pihak tidak jelas.	40	90	Diukur dengan skala Likert.
Kemampuan pengaduan	Peserta dapat menyusun kronologi sederhana jika data biometrik disalahgunakan.	60	90	Diukur melalui simulasi.



Gambar 1. Alur PKM Literasi Hukum Data Biometrik Pengguna Paylater

Gambar 1 menunjukkan alur pelaksanaan kegiatan yang menempatkan peserta sebagai subjek aktif. Peserta tidak hanya menerima materi, tetapi juga berlatih mengidentifikasi risiko, mengevaluasi legalitas pemrosesan data biometrik, dan menyusun langkah perlindungan mandiri.

4. Hasil dan Diskusi

4.1 Presentasikan Hasil

Hasil kegiatan PKM disusun berdasarkan capaian proses dan capaian pemahaman. Karena data lapangan perlu disesuaikan dengan pelaksanaan nyata, bagian ini menyediakan struktur pelaporan yang dapat langsung diisi oleh tim penulis. Secara proses, kegiatan diharapkan menghasilkan empat luaran utama: modul literasi hukum data biometrik, checklist legalitas pemrosesan data pada aplikasi paylater, template kronologi pengaduan, dan rekomendasi praktis bagi mitra. Luaran tersebut relevan dengan kebutuhan masyarakat karena isu perlindungan data pada paylater tidak dapat diselesaikan hanya melalui peraturan, tetapi juga membutuhkan kemampuan pengguna untuk memahami informasi, mengambil keputusan sadar risiko, dan menyimpan bukti secara tertib.

Pada tahap penyuluhan, peserta diarahkan memahami perbedaan data pribadi umum dan data pribadi spesifik. Data biometrik, seperti citra wajah yang digunakan untuk verifikasi identitas, harus dipahami sebagai data yang memiliki risiko tinggi. Apabila data tersebut bocor, pengguna tidak dapat menggantinya seperti mengganti kata sandi. Karena itu, peserta perlu memahami bahwa tombol setuju pada aplikasi bukan formalitas, melainkan dasar hukum yang harus diberikan secara bebas, spesifik, terinformasi, dan sesuai tujuan. Pemahaman ini menjadi fondasi perlindungan hukum preventif.

Pada tahap simulasi, peserta menilai kebijakan privasi dan izin akses pada aplikasi paylater dengan menggunakan checklist. Peserta diminta menguji empat pertanyaan: (1) apakah platform menjelaskan jenis data biometrik yang dikumpulkan; (2) apakah tujuan pemrosesan dijelaskan secara spesifik; (3) apakah tersedia informasi tentang jangka waktu penyimpanan dan pihak penerima data; dan (4) apakah terdapat mekanisme penarikan persetujuan atau penghapusan data. Simulasi ini membantu peserta membedakan antara pemrosesan yang wajar dengan permintaan data yang berlebihan.

Pada tahap klinik kasus, peserta dilatih menyusun kronologi apabila terjadi penyalahgunaan data, misalnya identitas dipakai untuk pengajuan pinjaman, akun paylater diakses pihak lain, atau foto wajah digunakan tanpa persetujuan. Kronologi minimal memuat tanggal kejadian, nama aplikasi atau pihak yang dihubungi, bukti notifikasi, tangkapan layar, bukti komunikasi, nomor laporan, dan kerugian yang dialami. Langkah ini penting karena perlindungan hukum represif membutuhkan bukti yang sistematis agar pengaduan dapat diproses secara efektif.

Tabel 3. Matriks Legalitas Pemrosesan Data Biometrik pada Aplikasi Paylater

Unsur Legalitas	Standar UU PDP	Risiko pada Paylater	Indikator yang Diperiksa Peserta
Dasar pemrosesan	Pemrosesan harus memiliki dasar hukum yang sah, seperti persetujuan atau pelaksanaan perjanjian.	Persetujuan tidak jelas, dipaksa, atau digabungkan dengan syarat lain tanpa penjelasan.	Ada notifikasi privasi; persetujuan dapat dibaca sebelum data dikirim.
Tujuan spesifik	Pemrosesan dilakukan untuk tujuan yang terbatas, jelas, dan sah.	Data wajah digunakan untuk tujuan lain, seperti pemasaran atau profiling berlebihan.	Tujuan e-KYC, keamanan akun, dan scoring dijelaskan secara terpisah.
Proporsionalitas data	Data yang dikumpulkan sesuai kebutuhan layanan.	Aplikasi meminta akses kontak, galeri, atau lokasi tanpa relevansi yang cukup.	Peserta membandingkan fitur yang digunakan dengan izin perangkat yang diminta.
Keamanan dan kerahasiaan	Pengendali wajib menjaga keamanan data pribadi dalam seluruh siklus pemrosesan.	Kebocoran data, akses internal tidak sah, atau penyimpanan tanpa enkripsi.	Ada penjelasan keamanan, kanal laporan, dan pemberitahuan insiden.
Hak subjek data	Pengguna memiliki hak atas informasi, akses, koreksi, penghapusan, dan penarikan persetujuan.	Pengguna tidak mengetahui cara meminta penghapusan atau koreksi data.	Tersedia menu bantuan, alamat pengaduan, dan prosedur permintaan hak.

Tabel 4. Rekomendasi Praktis Perlindungan Data Biometrik bagi Pengguna Paylater

Situasi	Langkah Preventif	Langkah Jika Terjadi Masalah
Sebelum mendaftar aplikasi paylater	Pastikan aplikasi terdaftar/berizin sesuai sektor jasa keuangan, baca kebijakan privasi, dan pahami data apa saja yang diminta.	Jangan lanjutkan registrasi jika aplikasi tidak jelas, meminta data berlebihan, atau menggunakan tautan di luar kanal resmi.
Saat melakukan verifikasi wajah atau swafoto	Pastikan verifikasi dilakukan di aplikasi resmi, jaringan aman, dan tidak mengirim foto wajah melalui chat pihak ketiga.	Simpan bukti permintaan verifikasi dan laporkan apabila ada permintaan swafoto dari nomor tidak dikenal.
Saat memberi izin akses perangkat	Aktifkan izin seperlunya, cabut izin yang tidak digunakan, dan periksa ulang menu privacy/permission.	Cabut izin akses, ubah kata sandi, aktifkan autentikasi ganda, dan dokumentasikan aktivitas mencurigakan.
Jika muncul tagihan tidak dikenal	Periksa riwayat transaksi secara berkala dan aktifkan notifikasi keamanan.	Hubungi layanan resmi, minta pemblokiran akun, susun kronologi, dan simpan semua bukti.
Jika data diduga bocor	Kurangi paparan data, jangan membagikan OTP, dan gunakan kata sandi berbeda untuk setiap aplikasi.	Ajukan permintaan penjelasan/penghapusan data, lapor ke kanal pengaduan platform, otoritas sektor jasa keuangan, dan aparat penegak hukum bila ada tindak pidana.

4.2 Diskusi Hasil

Diskusi hasil menegaskan bahwa legalitas pemrosesan data biometrik tidak dapat disederhanakan menjadi pertanyaan apakah pengguna telah menekan tombol setuju. Dalam konteks UU PDP, persetujuan harus dipahami bersama prinsip pemrosesan lain, seperti transparansi, tujuan spesifik, pembatasan pengumpulan data, akurasi, keamanan, dan akuntabilitas. Apabila aplikasi paylater mengumpulkan foto wajah untuk e-KYC, maka tujuan, jangka waktu penyimpanan, pihak yang menerima data, mekanisme keamanan, dan hak pengguna harus dijelaskan secara mudah dipahami. Tanpa informasi tersebut, persetujuan berisiko menjadi tidak bermakna.

Kegiatan PKM juga menunjukkan pentingnya membedakan perlindungan hukum preventif dan represif. Perlindungan preventif dilakukan sebelum terjadi kerugian, misalnya melalui literasi hukum, kebijakan privasi yang transparan, pengaturan izin akses, penggunaan enkripsi, audit keamanan, dan penilaian dampak perlindungan data. Perlindungan represif dilakukan setelah terjadi pelanggaran, misalnya melalui pengaduan, permintaan penghentian pemrosesan, permintaan penghapusan data, ganti rugi, sanksi administratif, dan proses pidana apabila terdapat perbuatan melawan hukum. Keduanya harus berjalan bersamaan karena perlindungan data biometrik tidak cukup mengandalkan penindakan setelah kebocoran terjadi.

Dari sisi pemberdayaan masyarakat, pendekatan penyuluhan partisipatif lebih tepat dibandingkan ceramah satu arah. Peserta perlu dilibatkan dalam menganalisis contoh notifikasi persetujuan, izin akses, dan kronologi kasus. Dengan cara tersebut, peserta tidak hanya mengetahui pasal dalam UU PDP, tetapi juga mampu menerjemahkannya ke dalam keputusan sehari-hari ketika menggunakan aplikasi. Hal ini sejalan dengan kegiatan sosialisasi terdahulu yang menunjukkan bahwa pemahaman peserta dapat meningkat ketika materi hukum disampaikan dengan metode pre-test, diskusi, simulasi, dan post-test (Bangun et al., 2023; Candiwan et al., 2025).

Dalam perspektif tata kelola platform, aplikasi paylater yang memproses data biometrik seharusnya menerapkan prinsip privacy by design dan security by default. Artinya, sistem sejak awal dirancang untuk meminimalkan data, membatasi akses internal, melindungi template biometrik, mencegah penggunaan ulang data di luar tujuan, dan menyediakan mekanisme penghapusan data. Kajian teknis mengenai teknologi pelindung privasi biometrik menunjukkan pentingnya perlindungan pada tahap akuisisi, ekstraksi fitur, penyimpanan template, pencocokan, hingga penghapusan data (Melzi et al., 2024). Dengan demikian, literasi pengguna perlu diimbangi dengan tanggung jawab platform.

Hambatan yang dapat muncul dalam pelaksanaan PKM adalah variasi tingkat literasi digital peserta, keterbatasan waktu untuk membedah kebijakan privasi yang panjang, dan kekhawatiran peserta untuk menceritakan pengalaman pribadi. Strategi mengatasinya adalah menggunakan bahasa non-teknis, studi kasus anonim, lembar checklist singkat, dan sesi konsultasi privat. Keterbatasan lain adalah bahwa program PKM tidak menggantikan proses pendampingan hukum formal. Oleh karena itu, tindak lanjut kegiatan perlu diarahkan pada penyediaan rujukan kanal pengaduan, penyimpanan bukti, dan konsultasi lanjutan dengan lembaga bantuan hukum atau otoritas terkait.

5. Kesimpulan

Data biometrik pengguna aplikasi paylater merupakan data pribadi bersifat spesifik yang memerlukan perlindungan lebih kuat karena melekat pada identitas seseorang, sulit diganti, dan dapat menimbulkan kerugian serius apabila disalahgunakan. Dalam perspektif UU PDP, legalitas pemrosesan data biometrik harus memenuhi dasar pemrosesan yang sah, tujuan yang spesifik, transparansi, proporsionalitas, keamanan, akuntabilitas, serta penghormatan terhadap hak subjek data pribadi. Oleh karena itu, proses verifikasi wajah atau bentuk biometrik lain pada aplikasi paylater harus dipahami sebagai aktivitas hukum yang memiliki konsekuensi bagi pengguna dan platform.

Program PKM yang dirancang melalui penyuluhan partisipatif, simulasi cek legalitas, klinik kasus, dan evaluasi pre-test/post-test dapat menjadi solusi pemberdayaan masyarakat. Program ini membantu peserta memahami haknya, mengenali risiko permintaan data berlebihan, mengatur izin akses perangkat, menyimpan bukti, serta menyusun kronologi pengaduan. Bagi mitra, kegiatan ini menghasilkan modul, checklist, dan model tindak lanjut yang dapat digunakan untuk edukasi berkelanjutan.

Rekomendasi dari artikel ini adalah: (1) platform paylater perlu memperkuat privacy notice yang mudah dipahami dan memisahkan persetujuan biometrik dari persetujuan umum; (2) pengendali data perlu menerapkan privacy by design, enkripsi, pembatasan akses, dan penghapusan data sesuai tujuan; (3) masyarakat perlu meningkatkan literasi hukum digital sebelum memberikan data biometrik; dan (4) kegiatan PKM berikutnya dapat memperluas sasaran ke pelaku UMKM, sekolah, komunitas mahasiswa, dan masyarakat rentan yang sering menjadi target penyalahgunaan identitas digital.

Daftar Pustaka

Bangun, B. H., Erwin, E., Kinanti, F. M., Wulandari, R., Sagio, I., & Darajati, M. R. (2023). Sosialisasi perlindungan data pribadi sebagai bagian dari hak asasi manusia. Jurnal Pengabdian Kepada Masyarakat Nusantara, 4(4), 3356-3365.

Candiwan, C., Prabowo, F. S. A., & Hidayatulloh, D. S. (2025). Sosialisasi perlindungan data pribadi berdasarkan UU No. 27 Tahun 2022 untuk para guru SMAN 5 Cimahi. Jurnal Pengabdian Masyarakat Akademisi, 4(3), 175-185.

Cornelli, G., Gambacorta, L., & Pancotto, L. (2023). Buy now, pay later: A cross-country analysis. BIS Quarterly Review, December 2023, 61-75.

Fadhli, Z., Rahayu, S. W., & Gani, I. A. (2022). Perlindungan data pribadi konsumen pada transaksi Paylater. Jurnal Hukum Magnum Opus, 5(1), 119-132.

Gunawan, I. (2024). Upaya preventif dan represif dalam penanggulangan kebocoran data pada penyelenggaraan pinjaman online. Officium Notarium, 4(1), 25-49.

Irawati, L., Hamzah, M. Z., & Sofilda, E. (2024). Regulating buy now pay later (BNPL) in ASEAN: A comparative analysis on regulatory challenges and opportunities. International Journal of Economics, Management and Accounting, 1(4), 60-81.

Kim, M. T., Jacob, Y. M. Y., & Bire, C. M. D. (2025). Perlindungan data pribadi pada platform digital pinjaman online ditinjau dari Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Studi kasus di Kota Kupang, NTT). Artemis Law Journal, 2(2), 511-526.

Kumar, A., Salo, J., & Bezawada, R. (2024). The effects of buy now, pay later (BNPL) on customers' online purchase behavior. Journal of Retailing, 100(4), 602-617.

Melzi, P., Rathgeb, C., Tolosana, R., Vera-Rodriguez, R., & Busch, C. (2024). An overview of privacy-enhancing technologies in biometric recognition. ACM Computing Surveys, 56(12), Article 310.

Novendra, B., & Aulianisa, S. S. (2020). Konsep dan perbandingan buy now, pay later dengan kredit perbankan di Indonesia: Sebuah keniscayaan di era digital dan teknologi. Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 9(2), 183-201.

Otoritas Jasa Keuangan. (2025). OJK issues buy now pay later practices regulation. Siaran Pers Otoritas Jasa Keuangan.

Ramadhani, A., Ramli, T. S., & Mayana, R. F. (2023). Pemanfaatan artificial intelligence pada fitur PayLater aplikasi Shopee dalam bidang e-commerce dikaitkan dengan data pribadi konsumen berdasarkan hukum positif Indonesia. COMSERVA: Jurnal Penelitian dan Pengabdian Masyarakat, 3(4), 1366-1379.

Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.

Safriadi, A. (2025). Perlindungan data pribadi konsumen Shopee Paylater di Kota Bukittinggi berdasarkan Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022. DATIN Law Jurnal, 6(1).

Sembiring, P. E., Ramli, A. M., & Rafianti, L. (2024). Implementasi desain privasi sebagai pelindungan privasi atas data biometrik. Veritas et Justitia, 10(1), 127-152.

Sitepu, G. A., & Fadila, A. (2024). Analisis pemanfaatan layanan Paylater di era keuangan digital oleh generasi Z. Journal of Young Entrepreneurs, 3(1), 57-70.

Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal data protection law in Indonesia: Challenges and opportunities. Indonesia Law Review, 14(2), Article 4.